СОВРЕМЕННЫЕ ТРЕНДЫ КИБЕРУГРОЗ И ТРАНСФОРМАЦИЯ ПОНЯТИЯ КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ СИСТЕМЫ ПРАВА

Карцхия А.А.[1], Макаренко Г.И.[2], Сергин М.Ю.[3]

Цель работы: *совершенствование научно-методических теоретических и правовых основ информационной безопасности.*

Метод исследования: *комплексный теоретико-сравнительный анализ действующего законодательства России и зарубежных стран в совокупности с анализом практики правоприменения.*

Результаты: *показаны особенности правового регулирования информационной безопасности в российском и зарубежном законодательстве, выделены основные свойства понятия кибербезопасность, в частности:*

– конфиденциальность данных (data confidentiality), то есть свойство, гарантирующее недоступность и закрытость данных;

– целостность данных (data integrity), т.е. свойство, гарантирующее сохранность данных, невозможность их изменения, уничтожения или утраты ввиду несанкционированных действий, несанкционированного извлечения информации (eavesdropping) или случайности;

– наличие криптографической защиты, шифрования текста с помощью криптографического алгоритма и ключа в целях сокрытия исходного смысла данных.

Ключевые слова: *киберпреступность,защита информации, правонарушения в информационной сфере, цифровые технологии, цифровые права, цифровизация права, информационно-коммуникационные технологии, стратегия развития.*

DOI: *10.21681/2311-3456-2019-3-18-23*

Современная глобальная стратегия мирового общественного развития определяется всеобщей идеей цифровой трансформации всех сфер повседневной жизни. В этих условиях особую актуальность приобретают вопросы кибербезопасности как отклик на современную «цифровую революцию», которая находит свое выражение в создании и бурном развитии современных цифровых, информационно-коммуникационных технологий, их широкого использования в различных сферах деятельности, и, как итог – в формировании «цифровой» экономики, «цифровизации» системы права. Современные цифровые и IT-технологии, включающие, в частности: Интернет вещей (Internet of Things), искусственный интеллект и современную робототехнику (AI & robotics), большие данные (Big data) и аналитику, облачные вычисления (Cloud computing), цифровое моделирование и дополненную реальность (augmented reality & simulation), аддитивное производство (additive manufacturing), – в своей совокупности и взаимосвязи создают технологический фундамент «цифровой экономики», новых социальных и общественных отношений в виртуально-цифровом пространстве. В современных условиях для повышения капитализации и получения конкурентных преимуществ бизнеса применяются новые цифровые промышленные технологии, которые определяются термином «Индустрия 4.0» и формируют новую четвертую мировую технологическую революцию – «цифровую революцию»[4].

Как показывают исследования последних лет, основой современного развития служат инновации, которые являются движущей силой общего роста[5].

В условиях «цифровой революции» сфера права преобразуется («форматируется») под влиянием возможностей современных цифровых технологий, что находит отражение, как отмечают исследователи феномена цифровизации права [1–9,16], во множестве новых правовых явлений, связанных с появлением новых субъектов и объектов правового регулирования, спецификой правоотношений в цифровой реальности, осмысления понятия и содержания цифровых прав и т.д. В частности, помимо традиционных субъектов права – юридических и физических лиц – в виртуальной, цифровой реальности

1 Карцхия Александр Амиранович, кандидат юридических наук, профессор РГУ нефти и газа (НИУ) им.И.М. Губкина, г. Москва, Россия. E-mail: arhz50@mail.ru

2 Макаренко Григорий Иванович, старший научный сотрудник ФБУ «Научный центр правовой информации при Минюсте России», г. Москва, Россия. E-mail: t7920518@gmail.com

3 Сергин Михаил Юрьевич, доктор технических наук, профессор, начальник отдела ФБУ «Научный центр правовой информации при Минюсте России», г. Москва, Россия. E-mail: mikhail.sergin@scli.ru

4 Digitalization for All Future-Oriented Policies for a Globally Connected World.G20, 2017. URL: https://www.b20germany.org/fileadmin/user_upload/documents/B20/ B20Digitalization_ Policy_Paper_2017.pdf; OECD Digital Economy Outlook 2017. OECD, 2017. URL: https://doi.org/10.1787/cc76d818/; Networks of «Things». NIST Special Publication 800-183. U.S. Department of Commerce, July 2016. URL: https://nvlpubs.nist.gov/nistpubs/Special Publications/NIST.SP.800-183.pdf

5 Global Innovation Index 2017: Innovation Feeding the World. Cornell University, INSEAD, the World Intellectual Property Organization (WIPO). Geneva,2017.URL:www.wipo.int/edocs/.

уже используются виртуальные (цифровые) личности как цифровой образ участников киберпространства (nick name, имя в сети Интернет), а также в вероятной перспективе появятся новые субъекты права – «электронные лица (персоны)» в виде искусственного интеллекта, андроида.

Развитие инфраструктуры, снижение стоимости обработки, хранения и передачи данных подводят человечество к порогу нового и наиболее масштабного этапа «цифровой революции». Сегодня вполне обосновано говорится о слиянии онлайн и офлайн сфер, о появлении киберфизического мира и формировании объективно нового явления, получившего название «Индустрия 4.0», которое характеризуется созданием и интеграцией принципиально новых революционных цифровых технологий.

Цифровые технологии оказывают сильное влияние на управленческие структуры, включая государственные органы управления. Формирование киберпространства и использование в нем новых технологий на базовом принципе распределенного (децентрализованного) реестра (blockchain tech) привело к созданию принципиально нового инструментария: умные контракты, электронно-цифровые подписи, базовые технологические патенты, стандарты и правила и т.д.

Как указывается в Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы[6] (далее – Стратегия), информационные и коммуникационные технологии, стали частью современных управленческих систем во всех отраслях экономики, сферах государственного управления, обороны страны, безопасности государства и обеспечения правопорядка. Для устойчивого функционирования информационной инфраструктуры Российской Федерации, как предусмотрено в Стратегии, необходимо обеспечить технологическую и производственную независимость и информационную безопасность, а для защиты данных в Российской Федерации необходимо также совершенствовать нормативно-правовое регулирование в сфере обеспечения безопасной обработки информации (включая ее поиск, сбор, анализ, использование, сохранение и распространение) и применения новых технологий, уровень которого должен соответствовать развитию этих технологий и интересам общества.

События последних лет, связанные с введением западными странами против России санкционного режима, а также политическими и военными кризисами в различных частях мира, которые наглядно показали критическую значимость систем информационной безопасности и кибербезопасности. В последние годы определился ряд устойчивых трендов существующих киберугроз.

В частности, российская компания Positive Technologies в результате мониторинга различных аспектов кибербезопасности в 2016 г. выявила следующие тенденции киберугроз, изложив их в итоговом документе[7]. В отчете отмечено, что результатом большинства компьютерных атак 2016 года стали утечки конфиденциальной и приватной информации. Основной целью большинства компьютерных атак стала компрометация данных (например, «утечка» множества учетных данных Yahoo, «ВКонтакте» и других массовых сервисов). Другой разновидностью стали целевые атаки «через человека — в корпорацию», направленные в основном на корпоративные активы. В последние годы такие атаки стали более скрытными. Популярным способом проникновения является социальная инженерия — таргетированный фишинг в виде делового письма. Именно с фишинговых писем начались и многие успешные атаки на финансовый сектор России, стран СНГ и Восточной Европы, включая атаку Cobalt. Только по открытым источникам, более 2 млрд. рублей похищены в 2016 году в ходе атак на российские финансовые сервисы.

Промышленные системы управления также продолжают быть объектом атак злоумышленников. Количество уязвимых компонентов промышленных систем управления из года в год не снижается, особенно это проявляется в области энергетики. В целом, среди найденных в сети Интернет компонентов АСУ ТП только две трети можно условно назвать защищенными.

Безопасность является наиболее актуальным вопросом в сфере современных информационно-коммуникационных технологий. К примеру, в докладе Европола за 2017 год «Оценка угроз организованной преступности в Интернете»[8] выделены особо опасные тренды киберпреступлений, к которым, в частности, относятся: разработка вредоносных компьютерных программ и средств (разработка «программ-вымогателей», банковские трояны и другие вредоносные программы (malware), организация DDoS-атак и ботов); кибератаки на критическую инфраструктуру экономики и государства (электростанции, транспортные узлы, объекты промышленности, объекты в системе Интернет-вещей и др.); Интернет-контент, касающийся сексуальной эксплуатации детей; террористическая активность в Интернете; мошенничество с банковскими картами и безналичными платежами; Интернет-торговля оружием, наркотиками иными запрещенными товарами, незаконная торговля людьми); он-лайн оборот контрафактной продукции и использование известных товарных марок (брэндов) в нелегальных Интернет-приложениях; мошенничество и кражи в отношении криптовалют, а также использование криптовалют (Bitcoin, Monero, Ethereum, Zcash) в киберпреступлениях и «отмывании» незаконных денежных средств; преступное шифрование данных; использование социальной инженерии в кибермошенничестве; трансграничный характер киберпреступности.

---

6 Указ Президента РФ от 09.05.2017 N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»//СЗ РФ, 15.05.2017, N 20, ст. 2901.

7 Кибербезопасность 2016–2017: от итогов к прогнозам. Positive Technologies, 2017.

8 Internet organized Crime Threat Assessment (IOCTA) 2017. European Union Agency for Law Enforcement Cooperation (Europol), 2017. pp. 10—12. URL:www.europol. europa.eu/

9 Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures. European Union Agency For Network And Information Security, November 2017. [Электронный ресурс] www.enisa.europa.eu. С.11-12, 19.

В докладе Европейского агентства сетевой и информационной безопасности (European Union Agency For Network And Information Security- ENISA) за 2018 год[9] отмечается, что угрозы и риски, связанные с устройствами, системами и услугами Интернета вещей, многообразны и быстро развиваются. Интернет вещей оказывает все большее влияние на безопасность и частную жизнь граждан, а сами виды угроз в отношении Интернета вещей чрезвычайно многообразны.

Для управления и снижения рисков, связанных с виртуальными активами, странам рекомендовано обеспечить регулирование оказания услуг с виртуальными активами на основе лицензирования или регистрации таких услуг и распространения на них эффективных систем мониторинга и соблюдения рекомендациях FATF. В Российской Федерации таким органом является Росфинмониторинг.

Путь цифровой трансформации требует фундаментальной перестройки подходов частного бизнеса и государства к взаимодействию, принятию решений, стимулированию инноваций и формированию, в том числе, цифровизации системы права, где у каждого участника системы – своя значимая роль.

Правительства развитых стран развивают амбициозные программы по созданию и совершенствованию цифровых сервисов для различных государственных услуг и даже целых сфер деятельности общества. В России это программа «Открытое правительство», функционирующее на основе Концепции открытости федеральных органов исполнительной власти[10], программа «Цифровая экономика Российской Федерации»[11].

В зарубежной практике примером может служить принятый правительством Великобритании в 2013 году и дополненный в 2016 году Свод практических правил (Technology Code of Practice)[12], который устанавливает стандарты (базовые правила) для взаимоотношений государственных структур с компаниями и физическими лицами при разработке, внедрении, а также продаже новых технологий.

В условиях высокой динамики развития ситуации и связанным с ним информационным фоном на первый план выходит задача создания эффективной защиты особо важных объектов и технологий, критической инфраструктуры в киберпространстве и обеспечение сохранности государственной, служебной и коммерческой тайны в глобальной информационно-коммуникационной среде.

Не менее важно укрепление международного сотрудничества в сфере кибербезопасности, которое сейчас начинает развиваться и на двусторонней основе между Россией и другими государствами (включая США, страны Европы, Китай, страны БРИКС. Создание более эффективной модели интернета, которая могла бы гарантировать суверенитет, безопасность и соблюдение принципов международного общежития в сочетании с соблюдением норм о неприкосновенности частной жизни, непосредственно связано с эффективностью охраны и защиты интеллектуальной собственности в киберпространстве [7–9].

В этой связи важно определиться с содержанием понятия кибербезопасности с учетом его трансформации в условиях цифровизации системы права.

В национальных стандартах Российской Федерации[13] кибербезопасность (киберзащита) (cybersecurity) применительно к любой системе в производственном процессе (включая независимые и связанные компоненты, коммуникация между которыми осуществляется с помощью внутренних сообщений, через разнообразные пользовательские или машинные интерфейсы, обеспечивающие аутентификацию, работу, управление или обмен данными каждой из таких систем управления) понимается как действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, имущественного ущерба и потери прибыли, а также повреждения критических систем или информационных объектов. При этом целью киберзащиты является уменьшение персональных рисков травмирования или угрозы здоровью населения, рисков потери доверия общественности или потребителей, разглашения информации о важных объектах, незащищенности бизнес-объектов или несоответствия нормативам. При этом понимании кибербезопасность включает в себя понятия идентификации, аутентификации, отслеживаемости, авторизации, доступности и приватности. Кибербезопасность (киберзащита) должна обладать рядом характерных свойств (отвечать ряду требований), и, в частности [10, 11]:

конфиденциальность данных (data confidentiality), т.е. свойство, гарантирующее недоступность и закрытость данных для любых неавторизованных субъектов системы, включая неавторизованных лиц, структуры или процессы;

целостность данных (data integrity), т.е. свойство, гарантирующее сохранность данных, невозможность их изменения, уничтожения или утраты ввиду несанкционированных действий, несанкционированного извлечения информации (eavesdropping), или случайности. При этом, подразумевается неизменность и конфиденциальность значений данных, но не их содержание или ненадежность источника значений;

наличие криптографической защиты, шифрования (криптографическое преобразование открытого текста в зашифрованный (закрытый) текст с помощью криптографического алгоритма и ключа в целях сокрытия исходного смысла данных во избежание разглашения факта их существования или использования) и эшелонирован-

10 www.open.gov.ru

11 Распоряжение Правительства Российской Федерации от 28 июля 2017 г. № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации»» // Сайт Правительства Российской Федерации. Режим доступа: http://government.ru/docs/28653. Дата доступа: 09.12.2018.

12 Technology Code of Practice (2016). http://www.gov.uk

13 ГОСТ Р 56205-2014/IEC/TS 62443-1-1:2009. Национальный стандарт Российской Федерации. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели. (утв. и введен в действие Приказом Росстандарта от от 10.11.2014 N 1493-ст), М.: Стандартинформ, 2014.

ной защиты (defence in depth) (наличие множественной, многоуровневой защиты и обнаружения угроз с целью предотвращения или сдерживания атаки);

целостность (integrity), т.е. свойство системы, отражающее логическую корректность и надежность операционной системы, логическую полноту аппаратного и программного обеспечений, которые реализуют защитные механизмы, а также постоянство структуры и содержания хранимых данных. Сюда включается также целостность в значении защищенности от несанкционированного преобразования или уничтожения информации (данных).

Киберзащита предполагает определенную архитектуру безопасности (security architecture), т.е. план и набор правил, описывающие сервисы безопасности, которые должна обеспечивать система для удовлетворения запросов ее пользователей, элементы системы для реализации таких сервисов, а также необходимые показатели эффективности функционирования элементов, воздействующих на угрожающую среду. Иными словами, архитектура безопасности представляет собой свод правил и набор мероприятий для реализации защиты управляющей сети от намеренных или случайных событий безопасности.

Реализация мер киберзащиты должна сопровождаться выявлением и управлением рисками (risk management) как вероятностным наступлением неблагоприятных последствий ввиду различных факторов внешнего или внутреннего свойства. Риск является функцией вероятности того, что данный источник угрозы, использует потенциальную уязвимость объекта защиты и закончится осуществлением воздействия этого неблагоприятного события на такой объект. В вышеуказанном национальном стандарте РФ риск (risk) определяется как ожидание ущерба, выраженное как вероятность того, что определенный источник угрозы воспользуется определенной уязвимостью системы, и это приведет к определенным последствиям.

Схожее определение риска приводится в Руководстве по управлению рисками для систем информационных технологий к Рекомендации Национального института Стандартов и технологий (США)[14]. В нем риск является отрицательным следствием наличия уязвимости и характеризуется, во-первых, вероятностью возникновения негативного события и, во-вторых, последствиями при возникновении этого события. Управление риском представляет собой процесс идентификации риска, процесс оценки степени риска и процесс осуществления мероприятий, направленных на уменьшение риска до приемлемого уровня.

Оценка риска (risk assessment) в соответствии с ГОСТ Р 56205-2014/IEC/TS 62443-1-1:2009 характеризуется как процесс систематического выявления потенциальных уязвимостей значимых ресурсов системы и угроз для этих ресурсов, количественной оценки потенциального ущерба и последствий на основе вероятностей их возникновения, и (в случае необходимости) разработки рекомендаций по выделению ресурсов для организации контрмер с целью минимизации общей уязвимости. При этом, ресурсы могут быть физическими, логическими, кадровыми и др. Оценки рисков часто бывают комбинированы с оценками уязвимостей, выполняемыми для выявления уязвимостей, и количественной оценкой связанных с ними рисков. Управление риском (risk management) представляет собой процесс определения и применения контрмер в соответствии со значимостью защищаемых объектов, на основе оценки риска Управление риском охватывает решение трех задач: оценка (или определение) риска, уменьшение риска, окончательные оценки и выводы [12, 13].

Важнейший аспект киберзащиты – применяемые меры защиты. Киберзащита проявляется в различных способах и мерах защиты, выражающих:

a) конкретные меры, предпринимаемые для защиты системы;

b) состояние системы, которое является результатом разработки и проведения мер защиты системы;

c) состояние ресурсов системы, защищенных от несанкционированного доступа к ним и несанкционированного или случайного их изменения, уничтожения или утраты;

d) возможность компьютерной системы гарантировать в достаточной степени защиту программного обеспечения и данных от изменения, несанкционированного доступа со стороны неавторизованных лиц и систем;

e) предотвращение несанкционированного или нежелательного проникновения, а также вмешательства в исправную и запланированную работу системы промышленной автоматики и контроля.

Такого рода меры представляют собой способы защиты, относящиеся к физической безопасности (управление физическим доступом к вычислительным объектам), или логической безопасности (возможность входа в конкретную систему и приложение).

В рассмотренных выше понятиях и характеристиках кибербезопасности акцент делается на киберзащиту, в то время как кибербезопасность - понятие более широкое по своему содержанию и значению, что и предопределяет его трансформацию.

Так, Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[15] определяет в ст.2 (п.2) безопасность критической информационной инфраструктуры как «состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак». Принципами обеспечения безопасности критической информационной инфраструктуры являются: 1) законность; 2) непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры; 3) приоритет предотвращения компьютерных атак.

---

14 NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. Gary Stoneburner, Alice Goguen, Alexis Feringa . URL:http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pd

15 Собрание законодательства РФ», 31.07.2017, N 31 (Часть I), ст. 4736

В результате преобразованное понятие кибербезопасности следует понимать как состояние защищенности объектов от разнообразных киберугроз. С точки зрения права, кибербезопасность представляет собой состояние защищенности в виде наличия достаточных адекватных мер и способов защиты прав и интересов субъектов права в киберпространстве, защиты от киберугроз (киберрисков) с помощью традиционных инструментов права (гражданского, уголовного, конституционного, административного, процессуального), так и с помощью новых способов с использованием возможностей современных цифровых IT-технологий.

Кроме того, трансформация понятия кибербезопасности должна учитывать также появление внешнеполитических угроз [14,15].

Как отмечается в п. 15 Стратегии научно-технологического развития Российской Федерации[16], одними из наиболее значимых с точки зрения научно-технологического развития Российской Федерации вызовами являются новые внешние угрозы национальной безопасности (в том числе военные угрозы, угрозы утраты национальной и культурной идентичности российских граждан), обусловленные ростом международной конкуренции и конфликтности, глобальной и региональной нестабильностью, и усиление их взаимосвязи с внутренними угрозами национальной безопасности. Реализация Стратегии научно-технологического развития Российской Федерации должна изменить роль науки и технологий в развитии общества, экономики и государства и привести, в том числе, к обеспечению роста влияния науки на технологическую культуру в России, повышению степени понимания политических, экономических, культурных, информационных и иных происходящих в современном обществе процессов и воздействующих на них разнообразных природных и социальных факторов, а также обеспечить повышение степени организации общественных отношений и содействовать предупреждению социальных конфликтов (п.36 «е»).

Таким образом, «цифровая революция» имеет глобальный масштаб, что предопределило и глобальный характер вопросов кибербезопасности, которые в своем понятии не ограничиваются статичными постулатами, а претерпевают динамичную трансформацию вместе с меняющимися трендами киберугроз и цифровизацией системы права.

Ввиду глобального характера проблем в киберпространстве и необходимости получения общих представлений о понятиях, угрозах и путях противодействия им Российская Федерация активно продвигает резолюцию по кибербезопасности в ООН. В ноябре 2018 г. Комитет Генеральной Ассамблеи ООН одобрил российский проект резолюции по разработке общеобязательных международных норм безопасности в киберпространстве.

Литература:

1. Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности // Журнал российского права, N 1, 2018. С. 85-102.
2. Понкин И.В., Редькина А.И. Искусственный интеллект и право интеллектуальной собственности // Интеллектуальное право. Авторское право и смежные права. № 2, 2018. С¬. 35-44.
3. Новоселова Л.А. «Токенизация» объектов гражданского права // Хозяйство и право, 2017, № 12.– С 29–44.
4. Карцхия А.А. Цифровые технологии – правовой аспект // ИС. Промышленная собственность, № 10, 2018. С.17-26.
5. Карцхия А.А. «Облачные» технологии: российское и зарубежное законодательство и практика правоприменения // Мониторинг правоприменения. № 2, 2018. С.36-41.
6. Карцхия А.А. Цифровизация в праве и правоприменении // Мониторинг правоприменения. № 1, 2018, с.36-40.
7. Карцхия А.А. Кибербезопасность и интеллектуальная собственность (ч.3) // Вопросы кибербезопасности. 2014. № 1 (2). С. 61-66.
8. Карцхия А.А. Кибербезопасность и интеллектуальная собственность (ч.3) // Вопросы кибербезопасности. 2014. № 2 (3). С. 46-50.
9. Карцхия А.А. Кибербезопасность и интеллектуальная собственность (ч.3) // Вопросы кибербезопасности. № 3, 2014 с. 59-66
10. Атагимова Э.И., Макаренко Г.И., Федичев А.В. Информационная безопасность. Терминологический словарь в определениях действующего законодательства / Федеральное бюджетное учреждение «Научный центр правовой информации при Министерстве юстиции Российской Федерации». Москва. 2017. (Издание 3-е). 448 с.
11. Барабанов А. В., Марков А. С., Цирлов В. Л., Рауткин Ю.В. Исследование уязвимостей программного обеспечения. монография / издание ФБУ «Научный центр правовой информации при Минюсте России». М, 2017. 76 с.
12. Ловцов Д.А. Системотология правового регулирования информационных отношений в инфосфере / монография. Москва, 2016.
13. Ловцов Д.А. Системология научных исследований / монография. Издание ФБУ «Научный центр правовой информации при Минюсте России». М, 2017. 76 с.
14. Гущина Е.А., Макаренко Г.И., Сергин М.Ю. Обеспечение информационно-технологического суверенитета государства в условиях развития цифровой экономики // Право.by. 2018. № 6 (56). С. 59-63.
15. Сергин М.Ю., Горбачёва Е.В., Макаренко Г.И., Танимов О.В. Концепция развития научной деятельности федерального бюджетного учреждения «Научный центр правовой информации при Министерстве юстиции Российской Федерации» // Правовая информатика. 2013. № 2. С. 4-11.
16. Bliznets, I., Kartskhiya, A., & Smirnov, M. (2018). Technology Transfer in Digital Era: Legal Environment. Journal of History Culture and Art Research, 7(1), 354-363. doi:http://dx.doi.org/10.7596/taksad.v7i1.1466

16 Указ Президента РФ от 01.12.2016 N 642 «О Стратегии научно-технологического развития Российской Федерации» // Собрание законодательства РФ, 05.12.2016, N 49, ст. 6887

MODERN TRENDS OF CYBER-THREATS AND TRANSFORMATION OF THE CONCEPT OF CYBERSECURITY IN THE CONDITIONS OF DIGITALIZATION OF THE SYSTEM OF LAW

Karzhia A. A.[17], Makarenko G. I.[18], Sergin M.Yu.[19]

The aim was to improve scientific and methodical theoretical and legal basic information programs.

The method of contrast: complex theoretical and comparative quality of the current legislation of Russia and foreign countries, together with the analysis of law enforcement practice.

Results: *The peculiarities of legal regulation of the information program in Russian and foreign legislation are shown, the basic properties of the concept of cyber security are highlighted, in particular:-Data confidentiality (data confidentiality) , there is a property that guarantees the unavailability and closure of the data;*

– Data integrity (data integrity), i.e. the property guaranteeing data safety, impossibility of gastroenterological passing, destruction or loss due to unsanctioned actions, unauthorized retrieval of entrant (eavesdropping) or randomness;

– Anti-Malware cryptographic protection, encryption of the text using a cryptographic algorithm and a key to conceal the original meaning of the data.

Keywords: *cybercrime, protection of the entrant, offences in information sphere, digital technologies, digital rights, digitization of Law, information and communication technologies, development strategy.*

References

1. Habrieva T.Ia., Chernogor N.N. Pravo v usloviiakh tcifrovoi` real`nosti // Zhurnal rossii`skogo prava, N 1, 2018. S. 85-102.
2. Ponkin I.V., Red`kina A.I. Iskusstvenny`i` intellekt i pravo intellektual`noi` sobstvennosti // Intellektual`noe pravo. Avtorskoe pravo i smezhny`e prava. № 2, 2018. S¬. 35-44.
3. Novoselova L.A. «Tokenizatciia» ob``ektov grazhdanskogo prava // Hoziai`stvo i pravo, 2017, № 12.– S 29–44.
4. Kartskhiya A.A. Tcifrovy`e tekhnologii – pravovoi` aspekt // IS. Promy`shlennaia sobstvennost`, № 10, 2018. S.17-26.
5. Kartskhiya A.A. «Oblachny`e» tekhnologii: rossii`skoe i zarubezhnoe zakonodatel`stvo i praktika pravoprimeneniia // Monitoring pravoprimeneniia. № 2, 2018. S.36-41.
6. Kartskhiya A.A. Tcifrovizatciia v prave i pravoprimenenii // Monitoring pravoprimeneniia. № 1, 2018, s.36-40.
7. Kartskhiya A.A. Kiberbezopasnost` i intellektual`naia sobstvennost` (ch.3) // Voprosy` kiberbezopasnosti. 2014. № 1 (2). S. 61-66.
8. Kartskhiya A.A. Kiberbezopasnost` i intellektual`naia sobstvennost` (ch.3) // Voprosy` kiberbezopasnosti. 2014. № 2 (3). S. 46-50.
9. Kartskhiya A.A. Kiberbezopasnost` i intellektual`naia sobstvennost` (ch.3) // Voprosy` kiberbezopasnosti. № 3, 2014 s. 59-66
10. Atagimova E`.I., Makarenko G.I., Fedichev A.V. Informatcionnaia bezopasnost`. Terminologicheskii` slovar` v opredeleniiakh dei`stvuiushchego zakonodatel`stva / Federal`noe biudzhetnoe uchrezhdenie «Nauchny`i` centr pravovoi` informatcii pri Ministerstve iustitcii Rossii`skoi` Federatcii». Moskva, 2017. (Izdanie 3-e). 448 s.
11. Barabanov A. V., Markov A. S., Tcirlov V. L., Rautkin Iu.V. Issledovanie uiazvimostei` programmnogo obespecheniia. monografiia / izdanie FBU «Nauchny`i` centr pravovoi` informatcii pri Miniuste Rossii». M, 2017. 76 s.
12. Lovtcov D.A. Sistemotologiia pravovogo regulirovaniia informatcionny`kh otnoshenii` v infosfere / monografiia. Moskva, 2016.
13. Lovtcov D.A. Sistemologiia nauchny`kh issledovanii` / monografiia. Izdanie FBU «Nauchny`i` centr pravovoi` informatcii pri Miniuste Rossii». M, 2017. 76 s.
14. Gushchina E.A., Makarenko G.I., Sergin M.Iu. Obespechenie informatcionno-tekhnologicheskogo suvereniteta gosudarstva v usloviiakh razvitiia tcifrovoi` e`konomiki // Pravo.by. 2018. № 6 (56). S. 59-63.
15. Sergin M.Iu., Gorbachyova E.V., Makarenko G.I., Tanimov O.V. Kontceptciia razvitiia nauchnoi` deiatel`nosti federal`nogo biudzhetnogo uchrezhdeniia «Nauchny`i` centr pravovoi` informatcii pri Ministerstve iustitcii Rossii`skoi` Federatcii»// Pravovaia informatika. 2013. № 2. S. 4-11.
16. Bliznets, I., Kartskhiya, A., & Smirnov, M. (2018). Technology Transfer in Digital Era: Legal Environment. Journal of History Culture and Art Research, 7(1), 354-363. doi:http://dx.doi.org/10.7596 / taksad.v7i1.1466

17 Alexander Karzhia, Ph.D., associate Professor, Professor University Gubkina, Moscow, Russia. E-mail: arhz50@mail.ru

18 Grigory Makarenko, Senior Research Fellow Federal Budgetary Institution «Scientific Center of Legal Information», Moscow, Russia. E-mail: monitorlaw@yandex.com

19 Mikhail Sergin , Dr.Sc., Professor, head of Department of Federal Budgetary Institution «Scientific Center of Legal Information», Moscow, Russia. E-mail: Mikhail.sergin@scli.ru